CLAIMS

1. (Original) A method of controlling access to execution resources comprising:

receiving a request to execute an instruction in a pre-boot environment;

determining an identity of the instruction;

determining if an access control list includes an entry corresponding to the instruction; and

selectively allowing the execution of the instruction if the access control list includes an entry corresponding to the instruction.

2. (Original) A method as defined by claim 1, further including allowing the execution of the instruction if a signature in the access control list matches a signature of the instruction.

3. A method as defined by claim 1, including selectively allowing the execution of the instruction if the access control list does not include an entry corresponding to the instruction if the instruction is signed.

4. (Original) A method as defined by claim 1, wherein the instruction is requested by a service call to be executed.

5. (Original) A method as defined by claim 4, including determining from the access control list system resources that may be used by the instruction.

6. (Original) A method as defined by claim 4, including determining an identity of an entity making the service call.

7. (Original) A method as defined by claim 4, including determining if the instruction to be executed is within a predefined area of memory.

8. (Original) A method as defined by claim 1, wherein the instruction is an operating system loader that dictates a secure boot and wherein a recovery mode of operation is entered if the access control list does not include an entry corresponding to the instruction.

9. (Original) An article of manufacture comprising a machine-accessible medium having a plurality of machine accessible instructions that, when executed, cause a machine to:

receive a request to execute an instruction in a pre-boot environment;

determine an identity of the instruction;

determine if an access control list includes an entry corresponding to the instruction; and

selectively allow the execution of the instruction if the access control list includes an entry corresponding to the instruction.

10. (Original) A machine-accessible medium as defined by claim 9, wherein the plurality of machine accessible instructions, when executed, cause a machine to allow the execution of the instruction if a signature in the access control list matches a signature of the instruction.

11. (Original) A machine-accessible medium as defined by claim 9, wherein the plurality of machine accessible instructions, when executed, cause a machine to selectively allow the execution of the instruction if the access control list does not include an entry corresponding to the instruction if the instruction is signed.

12. (Original) A machine-accessible medium as defined by claim 9, wherein the instruction is requested to be executed by a service call.

13. (Original) A machine-accessible medium as defined by claim 9, wherein the plurality of machine accessible instructions, when executed, cause a machine to determine from the access control list system resources that may be used by the instruction.

14. (Original) A machine-accessible medium as defined by claim 13, wherein the plurality of machine accessible instructions, when executed, cause a machine to determine an identity of an entity making the service call.

15. (Original) A machine-accessible medium as defined by claim 13, wherein the plurality of machine accessible instructions, when executed, cause a machine to determine if the instruction to be executed is within a predefined area of memory.

16. (Original) A machine-accessible medium as defined by claim 9, wherein the instruction is an operating system loader that dictates a secure boot and wherein a recovery

mode of operation is entered if the access control list does not include an entry corresponding to the instruction.

17. (Original) A system comprising:

an execution environment configured to execute code;

a instruction to be executed;

a platform security unit coupled to the execution environment and receiving a request to execute the instruction in a pre-boot environment, wherein the platform security unit is configured to: determine an identity of the instruction, determine if an access control list includes an entry corresponding to the instruction, and selectively allow the execution of the instruction by the execution environment if the access control list includes an entry corresponding to the instruction.

18. (Original) A system as defined by claim 17, wherein the platform security unit allows the execution of the instruction by the execution environment if a signature in the access control list matches a signature of the instruction.

19. (Original) A system as defined by claim 17, wherein the platform security unit selectively allows the execution of the instruction by the execution environment if the access control list does not include an entry corresponding to the instruction if the instruction is signed.

20. (Original) A system as defined by claim 17, wherein the instruction is requested by a service call to be executed.

21. (Original) A system as defined by claim 20, wherein the platform security unit determines from the access control list system resources that may be used by the instruction.

22. (Original) A system as defined by claim 20, wherein the platform security unit determines an identity of an entity making the service call.

23. (Original) A system as defined by claim 20, wherein the platform security unit determines if the instruction to be executed is within a predefined area of memory.